A Work Project, presented as part of the requirements for the Award of a Master Degree in Management from the

NOVA – School of Business and Economics

„The Impact of Blockchain Technology on the Trustworthiness of Online Voting Systems“

–

„An Exploration of Blockchain Technology“

Ivo Konzok – 34239

A Project carried out on the Master in Management Program,

under the supervision of:

Prof. Andrew Bell

Lisbon, 6 January 2020

„The Impact of Blockchain Technology on the Trustworthiness of online Voting Systems“ – „An Exploration of Blockchain Technology“

Abstract

Online Voting evidently increases election turnouts. However, recent state-owned initiatives have failed due to security concerns and a lack of trust in the systems. Blockchain seems to be a very suitable technical solution to establish transparency in online voting and thus, create trust. We have built our own, blockchain-enabled voting platform and utilized it to run an A/B-testing experiment at an university election to investigate its effect. Our results show that students trusted the blockchain-based voting version less than the control version. However, literature and our focus group findings revealed that there is an interrelation between the distrust among the students and a low level of familiarity with blockchain technology. Hence, we conclude that people should be educated before being confronted with blockchain-enabled online voting to take advantage of the technology's potential.

Keywords: Blockchain, Online Voting, Trust, Transparency

This work used infrastructure funded by Fundacao para a Ciencia e a Tecnologia (UID/ECO/00123/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209)

Table of Contents

Table of Figures **3**
Table of Tables **3**

1. Introduction **4**

Individual Contribution **5**
2 Literature Review **5**
2.1 Definition, categorization and technical functionalities .. **Error! Bookmark not defined.**
2.2 Limitations of blockchain technology 11
2.3 Economic and public applications 13

Group Contribution **15**
3. Discussion **15**
3.1 Empirical results ..... **Error! Bookmark not defined.**
3.1.1 Main findings 16
3.1.2 Subgroup findings 19
3.2 Focus froup findings 20
3.3 Limitations ..... **Error! Bookmark not defined.**
3.4 Future research ..... **Error! Bookmark not defined.**
3.5 Lessons for practitioners ..... **Error! Bookmark not defined.**

4. Conclusion ..... Error! Bookmark not defined.
5. Bibliography **30**

Table of Figures

Figure 1: Blockchain illustration.....7

Table of Tables

Table 1: Selected properties and principles of blockchain technology.....5

1. Introduction

According to Russell and Zamifir (2018), participation rates in parliamentary elections dropped by more than 10% globally between 1980 and 2018. To take countermeasures against this trend, online voting turned out to be a promising idea. Breux et al. (2017) found evidence that online voting actually increases election turnouts by especially encouraging less committed voters. Unfortunately, various, state-run initiatives to implement online voting have failed. The Netherlands forbade electronic counting of votes due to a strong fear of cyberattacks (Lowe, 2019) and France stopped all ongoing initiatives because of similar motivations (Reuters, 2017). The only exception remains Estonia, which already enabled online voting in parliamentary elections since 2005. In 2019, for the first time in history, it became the most popular channel to cast a vote with 44% of all participating voters using it (Krivonosova, 2019).

However, what seems to be missing to expand the implementation of online voting systems is the right technology. Both, the responsible authorities and the broad population have to trust their voting system to enable a successful transformation. Spycher et al. (2011) identified transparency as the most crucial factor for establishing trust in online voting systems. In achieving this, Dogo et al. (2018) stress that blockchain technology establishes strong perceived transparency. Our implied research hypothesis therefore states that introducing blockchain technology to online voting system does actually increase the trust in this system. This hypothesis turns into our research question: To what extent the use of blockchain technology actually impacts the trustworthiness of online voting systems?

With the goal of investigating the answer, we built our own, blockchain-based online voting system, called Votechain, to run an expedient experiment. It technically works on a blockchain protocol and enables voters to cast their ballot online and verify it afterwards. Hereby, the voters are given access to the entire blockchain of the particular election they are participating in, in an encrypted manner. Each block represents one vote.

Votechain has been utilized in a students' elections encompassing almost 1000 votes out of which roughly every second student actively participated in our A/B-Testing experiment. The main goal of this experiment was to investigate, whether students who were prompted with a visualization of the election blockchain after they cast their vote would actually trust this online voting system more than the control group, to which state-of-the-art security methods were shown instead.

Our research paper starts off with an extensive literature review including an elaboration about the nature of elections, voting methods and the transition to online voting (1), blockchain technology (2) and blockchain-based voting (3). Thereafter, we describe Votechain and our experiment in the methods, present the experiment's results in the results section as well as adequate statistical analysis and put these results in the context of our research questions in an extensive discussion and conclusion.

Individual Contribution

The literature review is split into three sections and represents the individual contributions to the master thesis of all of the team members. Nina Vysna created the first section — *Elections and trust* — which she submitted individually and Ivo Konzok developed the second — *An exploration of blockchain technology* — which is part of the overall submission in this document. The third section — *Blockchain-enabled online voting* — is written by Kevin Riedlberger and was submitted individually as well.

2. Literature Review

Nakamoto (2008) was the first to explain blockchain technology when he introduced the Bitcoin System. Although Bitcoin remains among the most well-known blockchain applications, the underlying technology is applicable in many other systems, institutions and whole industries.

This chapter starts by defining blockchain, classifies it, explains technicalities and stresses the most troubling limitations. It concludes with relevant blockchain uses for both, economic and public purposes. Since our research contribution focuses on the impact blockchain has and could potentially have on online voting, this chapter incorporates relevant details about deciding factors regarding this matter.

2.1 Definition, categorization and technical functionalities

A blockchain is a widely distributed public ledger system. It is recorded and stored across many computers (Akcora et al., 2018). Since all computers store the same copy of timestamped documents, nobody can manipulate their content without recognition (Di Pierro, 2017). Before a new set of information can be added to the blockchain, the network of computers must reach consensus about its correctness. In the context of blockchain, documents are called transactions and are bundled in blocks (Akcora et al., 2018). Transactions do not have to be financial but can contain very different kinds of metadata. Precisely, they can be any exchange of information like a vote or any exchange of property like real estate (Veuger, 2018).

Twesige (2015, p. 4) adds a broader, purpose-driven approach of defining Blockchain by explaining that it is a "protocol that governs the rules and regulations for value exchange". Since there are no commonly accepted definitions of the features implicit in blockchain (Zile et al., 2018), we selected relevant properties as provided by Iansiti and Lakhani (2017) and underlying principles as stated by Wang et al. (2018) to substantiate the nature of blockchain.

Table 1 lists all properties in the descending order of relevancy and links them to their respective, underlying principle.

Table 1: Selected properties and principles of blockchain technology.

Property	Underlying Principle
Decentralisation: Disappearance of central intermediaries.	**"Peer-to-peer transmission"**: Refers to the implemented consensus algorithm[1] which ensures autonomy.
Persistency: Refers to transactions having to be confirmed by the whole network to be validated and eventually conducted.	**"Irreversibility of records"**: Transactions are not invertible once approved by the network since every transaction is part of a block which links back to all blocks that came before it on the chain.
Anonymity: Identification information of network members are replaced by systematically generated public keys, which are 30-plus-character alphanumeric addresses.	**"Transparency with pseudonymity"**: It means that each user is identified with the aid of its public key. Public keys are visible to the entire network. Transactions occur directly between them.
Auditability: Transactions contain a timestamp allowing nodes to trace all previous records.	**"Distributed database"**: All nodes store a duplicated version of the entire blockchain.
Transparency[2]: The entire history of transactions can be seen by all nodes.	**"Distributed database"**: All nodes store a duplicated version of the entire blockchain.
Tamper resistance[2]: It is worth noting that the extent to which a blockchain is tamper-resistant depends on the network size. The level of security increases with the size because blocks cannot be overwritten and have to be created newly in case of an attack**.**	**"Irreversibility of records"**: Transactions are not invertible once approved by the network since every transaction links back to all records that came before it.

To briefly examine transparency as a key property of online voting systems (Spycher et al., 2011), Iansiti and Lakhani (2017) derive blockchain's potential to enhance their transparency from the fact that the entire history of cast votes would be stored on the blockchain, visible to the entire network.

[1] Consensus algorithms are systematically implemented mechanisms used to validate transactions to maintain the chain's immutability (Wang et al., 2018).
[2] Tamper resistance and transparency have been added to the list by Viriyasitavat and Hoonsopon (2019).

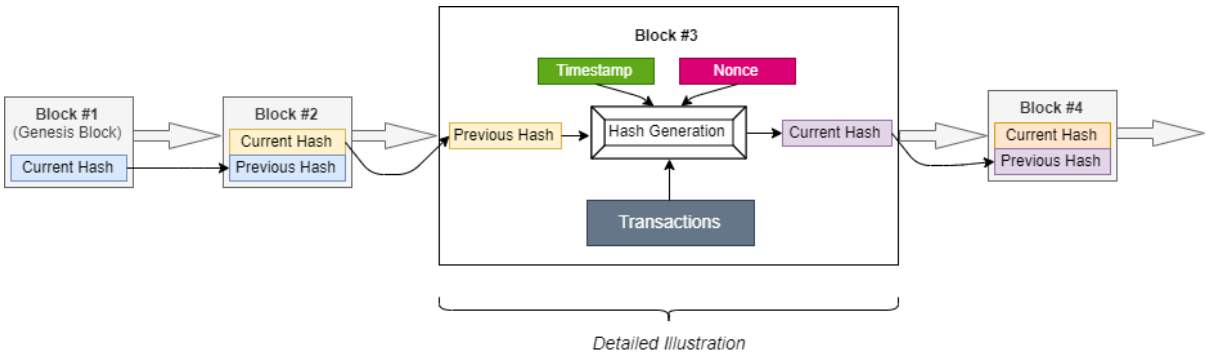
Osgood (2016) adds that every stakeholder is able to check specific details. Because of this, a blockchain-based online voting system would not have a single point of failure and every voter could independently verify the computational transcript of single votes. Benchoufi et al. (2017) broadens the perspective by stressing that we live in increasingly informed societies. Thus, distributing fractions of trust through a network could counter the growing mistrust in institutions like centralised banks or election authorities.

Buterin (2015) classifies three different types of blockchains: Public blockchains, private blockchains and consortium blockchains. These three types differ in who is able to access the blockchain, pass transactions to it and contribute to its consensus algorithm (Wang, 2019). Public blockchains are publicly readable and accessible which potentially attracts a high number of nodes. Large networks result in highly tamper-resistant chains, demonstrating an important strength of public blockchains. Conversely, the larger the network size the lower its operational efficiency, indicating a clear weakness of public blockchains. A private blockchain is partially centralised since read permission can be restricted. It solely consists of trusted nodes, which are verified and invited network members, as well as an owner who controls access. Consequently, private blockchains suit systems for bounded communities like institutions (Viriyasitavat and Hoonsopon, 2019). Lower network computing power goes along with a higher level of control which leads to increased efficiency but higher vulnerability for being tampered. Lastly, consortium blockchains include rigorously selected main nodes which have specific network authorities. They can be applied to many business use cases like Hyperledger, which was created to use blockchain for industrial purposes (Akcora et al., 2017). These blockchains are entirely centralised, restrict public read permission and suit organized systems consisting of multiple organizations (Viriyasitavat and Hoonsopon, 2019).

To begin the technical explanation of blockchain's functionality, it is worth noting that it provides a large variety of applications like cryptocurrencies (Nakamoto, 2008), financial transactions (Apte and Petrovsky, 2016) and online elections (Crosby et al., 2016). However, regardless of the intended utilization, the technical functionality is always relatively similar and bases on transactions being propagated through the network.

Once approved, transactions are bundled into blocks. Blocks do not only contain a set of systematically approved transactions but a timestamp, the hash value of the previous block (parent block) and a nonce, which is a randomly generated number for verifying the hash (Nofer et al., 2017). Figure 1 shows a graphical illustration of this interrelated series of blocks.

Figure 1: Blockchain illustration.



The hash value is calculated by a hash function which transforms large data inputs into small target data and generates the hash value as a checksum to verify this data (Giese et al., 2016). Every blockchain starts with an initial block, called the Genesis block, containing the initial transaction. The verification of newly proposed transactions works along the mining process which is the mechanism to attach new blocks to the chain. The moment in time when there is consensus for a newly proposed transaction, is called Byzantine Fault Tolerance (Dogo et al., 2018). Its progress depends on the respective consensus algorithm the blockchain uses.

Concerning consensus algorithms, Bitcoin uses Proof-of-work (PoW), other blockchains use alternatives like Proof-of-Stake (PoS), as illustrated by Akcora et al. (2017) and specified by Wang et al. (2018). The intuition behind consensus algorithms is to use a nodes' self-interest to establish a secure mechanism to verify transactions (Bauerle, 2019a). All algorithms require miners to prove that they have contributed sufficient computational power to the network, called work, to generate a block. The pay-off for miners is that they receive rewards, often monetary, for properly mining blocks. This mechanism ensures blockchain's autonomy and its tamper resistance, since all deployed work from the genesis block up to the latest block on the chain must be repeated to conduct any modifications to a block's content. The reason for this is that each block's hash is linked to the block before it. Therefore, to be able to influence the character of ongoing, newly added blocks, an attacker would have to outpace all of the ongoing work (Nakamoto, 2008).

To further illustrate transaction processing, we follow an example. Suppose Bob (Transaction sender) wants to send one Bitcoin (BTC) to Sally (Transaction receiver). Sally is able to access the received input with the help of the Private Key, which is a randomly generated 256-bit number and always exists as a key pair together with the Public Key. Once Sally (Receiver) accessed the transaction input (One BTC), she can use it or any smaller amount to send it to another public key (user's address) in the network, thus act as a sender. Every transaction input can solely be used once. If Sally sends any smaller amount than one BTC, two transactions are generated ("Common Transaction"). One to send the initiated output to the receiver and a second to return the remaining amount to Sally (Lánský, 2017).

Wang (2019) summarizes three main blockchain applications: Decentralized currencies (such as Bitcoin), self-executing contracts called Smart Contracts and smart property which refers to assets or information that can be directed over the Internet.

Concerning the latter two use cases, we should introduce Ethereum, the second largest existing blockchain after Bitcoin. Ethereum relies on the largest existing developer community within the blockchain sector as well as massive industry awareness (Trustnodes, 2017). It's main advantage against Bitcoin lies in scalability. Ethereum achieves around 15 transactions per second (Hertig, 2019a) whereas Bitcoin is limited to approximately seven (Bauerle, 2019b).

Ethereum was particularly created for executing Smart Contracts, initially introduced by Szabo (1997). Wang (2019, p. 14) defines Smart Contracts as "a computerised transaction protocol that automatically executes the terms of a contract upon a blockchain".

According to Hertig (2019b), smart contracts mainly support four functions. First, they work as "multi-signature" accounts, which means that agreed transactions are only spent if a required share of people agrees. Second, they manage user agreements. Third, smart contracts can overtake parts of other, extensive contracts. The author compares this functionality to software libraries. And fourth, users can store information on smart contracts, such as member records or application details.

2.2 Limitations of blockchain technology

Before discussing limitations of blockchain technology, it is important to stress the overall limitation of evidence-based literature in this research area. Research surrounding blockchain technology is still very young (Wang, 2019).

Wang et al. (2018) summarize four main problem areas. First, the lack of scalability. As an example, Bitcoin must confront its transaction processing limit. Two resolution approaches have been proposed: first, Bruce (2014) proposed a storage optimization for the Bitcoin blockchain, in which a shortened *Mini blockchain* is secured by a *Proof Chain*. Second, Eyal et al. (2016) reshaped Bitcoin's block structure with the help of their *Bitcoin-NG* (Next Generation) approach. However, it is worth noting that neither of these approaches have been tested extensively.

The second major limitation of blockchain technology is, selfish mining, which occurs when nodes do not publish their readily mined blocks but withhold them to gain increased earnings when these blocks are eventually published to the network.

The third problem area lies in problematic consensus algorithms with respect to speed and energy consumption. According to Stoll et al. (2019), Bitcoin's PoW has an average energy consumption of 45,8 TWh per annual. A single Bitcoin transaction therefore requires more energy than 100.000 VISA transactions (Digiconomist, 2019).

A fourth issue surrounds privacy damage. Barcelo (2014) shows that Bitcoin transactions can be linked to user information which can then possibly be linked to IP addresses meaning a loss of users' anonymity (Biryukov et al., 2014). The possibility of a loss of anonymity might weaken the general security of blockchain infrastructures. For instance, online voting systems put great weight on security as a key property of blockchain, both to protect voters and to secure the correctness of the election result (Dogo et al., 2018). Again, two relativising remarks must be stated. First, this evidence is solely based on the Bitcoin blockchain and requires further research to determine whether it can be a risk for other blockchain applications either. Second, many attempts have been published to solve these security issues although none of them was implemented successfully so far.

To add a less technical perspective, Iansiti and Lakhani (2017) compare blockchain's implementation to previously implemented technical revolutions like the Internet and conclude that various governmental and societal concerns still have to be overcome.

Hence, blockchain-based applications have to comply with functionality standards of traditional alternatives or be suitable for the respective ecosystem they aim at being implemented in.

2.3 Economic and public applications

Blockchain has many uses beyond cryptocurrencies, and researchers and entrepreneurs have already been implementing the technology into public and economic services, supply chain management, Internet of Things (IoT) and reputation systems. This review will explore many of these implementations.

Within the area of economic services, the literary focus often lies on financial applications like cryptocurrencies or infrastructure improvements of the finance sector. This includes traditional banking, security issuance, trading or risk management (Jaag and Bach, 2017; Miraz and Ali, 2018; Crosby et al., 2016). Other economic services can be related to managing right ownership within the music industry (Crosby et al., 2016; Nofer et al.,2017). Legal documents would be timestamped and published to the blockchain in the form of a transaction. Changes can be noted in blocks following on the chain so that the up-to-date status is unchangeably visible for the whole network. Furthermore, the increasingly important Blockchain-as-a-Service (BaaS) sector builds private blockchains to be accessed online. Firms like Amazon Web Services or Microsoft Azure provide their clients with preformatted blockchain environments to be individually adapted according to clients' needs (Amazon Web Services, 2019; Microsoft Azure, 2019).

Concerning public uses, blockchains can improve postal services, social services like registration processes, notary issues or digital content rights management (Crosby et al., 2016; Wang et al., 2018; Jaag and Bach, 2017). A very pictorial example is contract authorization by notaries, which becomes needless since all changes to the ownership of assets like real estates could be stored and updated on a blockchain. For instance, instead of the notary verifying ownership changes, they are consecutively transmitted via transactions and confirmed as well as transparently stored by the entire network of nodes, provided by the responsible authority (Nofer et al., 2017).

Dodo et al. (2018) stress the perceived security and transparency of blockchain applications which underscore their potential in online voting. Hjalmarsson et al. (2018), among others, propose a blockchain-based electronic voting system that is using smart contracts to cast and process votes. By leveraging an Ethereum private blockchain the authors were able to create a highly scalable system, overcoming the scalability limitation mentioned before. Other promising initiatives, which try to leverage blockchain protocols to create online voting applications are explored in the following section of our literature review.

The second application area, supply chain management, is investigated by Boucher et al. (2017) who conducted an in-depth analysis for the European Parliament, measuring blockchain's impact on human lives. According to the authors, blockchain possibly offers infrastructure for registration, certification and tracking processes between economic parties which in turn provides the necessary trust through embedded properties like timestamping. According to Wang (2019), a product's origin could be examined immediately by implication since every movement would be tracked by GPS sensors and simultaneously sent to the chain. Smart contracts can automate payments to suppliers as soon as products arrive at their destination, thus increasing efficiency and reducing costs.

Concerning IoT, blockchain's greatest benefit lies in ensuring data integrity (Liang et al., 2017). Since it can track data provenance and makes centralized, data storing servers obsolete, a blockchain system ensures secure communication between machines in an IoT environment. Filament, a company combining the Bitcoin and Ethereum blockchain with IoT solutions, impressively shows these benefits (Rizzo, 2015). It developed an application, which features real-time data processing leading to automatic interaction between devices based on autonomous smart contracts (Pajot-Phipps, 2017). To list a few more promising solutions combining both technologies, Liang et al. (2017) describe how data integrity allows secure exchange of data between drones.

The IBM Watson platform already enables users to store specific IoT related information in private blockchains by transforming their format so that smart contracts between multiple devices can be processed.

Referring back to blockchain's ability to ensure trust between parties due to data integrity, reviews could be authenticated as well, thus avoiding falsification of ratings (Wang et al., 2018). To provide two examples, Yang et al. (2017) used blockchain technology to develop a reputation system for vehicular networks to ensure the reliability of communicated messages. Schaub et al. (2016), on the other hand, developed a blockchain-based reputation verification system to warrant the credibility of reviews on E-Commerce platforms, which play a key role in driving purchase decision (Kim and Srivastava, 2007). While all these applications should be mentioned and kept in mind when evaluating the opportunities blockchain provides for our society, the main focus of our research contribution is its suitability for and impact on online voting. Therefore, the following section compares traditional and online voting, highlights why blockchain can improve the latter and evaluates existing initiatives.

Group Contribution

The following discussion refers to the findings of our overall project which is explained in Riedlberger (2020) and whose results can be found in Vysna (2020).

3. Discussion

Our research hypothesis states that the implementation of blockchain technology in online voting systems will increase their trustworthiness. To test blockchain's impact, we ran a randomized A/B test in the Nova SBE Student Representatives elections 2019, with a total turnout of 967 participants. Voters were asked to fill out a survey attached to the voting process. The survey answers showed how the two sample groups, A and B, differed in their perceived trust in our online voting system. We administered the 'Trust in a specific technology' framework designed by McKnight et al. (2011) which consists of three layers.

These layers are, in ascending order of detail, trust in general technology, trust in a class of technology and trust in a specific technology, the latter being blockchain-based online voting system in this case. These three constructs can be divided into sub-constructs as has been explained in the methods section.

Before focusing on the results of our experiment, we want to briefly elaborate on the turnout of the particular election we ran our experiment on. As we have illustrated in the results section (Figure 3), this year's student representative election at Nova SBE exhibited a four times higher voter turnout as compared to the previous year. While the outcome can be attributed to several reasons such as reminder emails or the survey incentive, we believe that the convenience of the application's online voting process compared to formerly used paper-ballots, also contributed to the increase in turnout. To initiate the discussion of our findings we subdivided this chapter into five paragraphs, namely empirical results (5.1), focus group findings (5.2), limitations of our research (5.3), future research suggestions (5.4) and lastly, key lessons for practitioners (5.5).

3.1 Empirical Results

We will start with an analysis of our main findings (5.1.1) and complement it with an elaboration on subgroup results (5.1.2).

3.1.1 Main findings

Our main result, despite the initial hypothesis, suggests that there was no improvement in trust when using a voting system based on blockchain technology. In fact, the opposite was true - our results showed that students who were prompted with two-factor authentication security instead of a blockchain script felt more confident that the system works reliably and that their vote was cast correctly.

Although there was no significant difference in six of the seven trust sub-constructs composing the administered framework, the first regression model we applied showed that the reliability score was significantly higher in group A than it was in group B. We therefore failed to reject the null hypothesis.

The most logical explanation for this counterintuitive outcome is that people are more familiar with two-factor authentication, applied in many online banking applications, than they are with blockchain technology. To incorporate a psychological perspective, Luhmann (1979) claims that familiarity is a precondition for trust, which supports this explanation. Our focus group discussion revealed evidence for this argument. For instance, subject 5 clearly stated: „But I do not understand blockchain and how it works, […] because I do not understand it, I do not trust it." – Associated therewith, a higher level of familiarity seems to enable students to develop a higher level of trust, as Subject 1 indicated: „But someone explained to me how blockchain is actually working and I think […] that the risk of losing votes is even less [when using blockchain protocols] because in the EU election where they counted the votes traditionally, they also had miscounted votes."

A second possible justification arises from the design difference between the verification webpage for control group A and the blockchain-based group B. While voters were informed about the implemented usage of two-factor authentication in written format, we additionally showed visualizations of the election blockchain in version B (see appendix 6 and 7 for screenshots of both versions). Since people tend to differ in their comprehension of written or visual information format and understanding the blockchain visualization could have required more time exposure or higher technology affinity than the explanatory text in version A, this might have influenced our results. This effect could have been increased even further by the combination of the Student Representatives Election's relatively low importance and the high complexity of a blockchain-based system.

Students potentially did not make the effort to understand the visualization, especially without prior knowledge about the technology. Someone who is not interested in the functionality of the system when casting a vote could be overwhelmed by a blockchain visualization rather than a short, explanatory text and thus, conclude that the system is complicated or less reliable. An indication that the blockchain visualization might have indeed been overwhelming, is relatively lower survey participation in the treatment group (43.8 %) than in the control group (50.1 %).

Regarding the applied 'Trust in a specific technology' framework by McKnight et al. (2011), our findings further show that voters' survey answers do not imply any significant difference in their scores on the construct level - general trust in technology, a class of technology or a specific technology. This fact enables us to neglect any biases in survey answers arising from significant differences between people's general attitude towards technology. Additionally, the second applied regression model confirmed the proposition of McKnight at al. (2011) who suggested that there is a direct relationship between institution-based trust and trust in specific technology. In our case, that would mean that if one is familiar with online election systems, perceive them as trustworthy and believes that there is enough structural support around these systems, one is more likely to trust our voting application. This was indeed exhibited in the results as subjects with low and neutral institution-based trust rated our voting application (regardless of its version) significantly lower than subjects with high institution-based trust.

In addition, McKnight et al. also found a direct relationship between trust in general technology and trust in specific technology. In our case, if one has generally higher trust towards IT, one should also exhibit more trust in our application. This effect was pronounced more for the blockchain version of the app.

Subjects who received the blockchain version of the app and have a neutral propensity to trust general technology, evaluated functionality, helpfulness and overall trust in the blockchain voting system significantly worse than those with high general technology trust and two factor authentication version. This might indicate that blockchain technology is more suitable to be implemented in the contexts where election participants are rather tech-savvy and thus have high trust in technology in general.

To mention some of our non-significant findings, the results revealed no significant difference in six of the seven tested sub-constructs. To highlight *helpfulness*, a possible explanation for this insignificant outcome is that voters simply did not use Votechain long enough to encounter relevant problems for which the help function could have provided required support. None of the interviewed students of our focus group study used the help function either. On the other hand, this findings might also imply that our design approach met the students‘ expectations for the limited scope of an university election and thus, students felt well supported when voting in both versions.

To conclude, our voter sample seems to trust two-factor authentication and blockchain technology as possible means to secure online voting systems equally, with the only exception that they perceive two-factor authentication systems as being slightly more reliable.

3.1.2 Subgroup results

Before stressing a few examples, we have to mention that our results did not imply any meaningful differences among analysed sub-groups gender, nationality and program. Due to the lacking variation in the age and race of our subjects, we did not include these variables in the subgroup analysis. As discussed in section 5.3, our sample consisted of predominantly white students aged 18-24, either Portuguese or German and enrolled in business and economics degrees.

Concerning gender, we observed that male and female students came to very similar conclusions in terms of specific technology trust and institution-based trust. This is somewhat surprising considering the existing literature that suggest that there are certain differences between the two genders regarding their perceptions of information technology. Shaouf and Altaqqi (2018) summarized previous research on gender differences in adoption and use of IT and found that men are generally more likely to try new technologies, evaluate websites more positively and to trust websites more than women. Our results actually suggest the opposite, females scored significantly higher on the faith in general technology sub-construct than males, regardless of the version.

A second sub-group finding was that PhD students had a significantly lower score on reliability, helpfulness and trusting beliefs in specific technology, as has been stated in the results chapter (model two). While this effect is independent from the version of the application, it still means that PhD students exhibited a lower level of trust towards our online voting system than Master students. This finding would suggest that people with higher education are less likely to trust an online voting application. However, since our sample size of PhD students was very limited (22 students), we are not able to draw strong conclusions at this point. It is also rather difficult to support the finding with existing research. As mentioned in the literature review, some studies showed that young and highly educated voters tend to have higher affinity with IT which positively influence their trust in e-voting, while other studies suggested the opposite – higher educated people as well as young people tend to know more about technology hence, they are also aware of its vulnerabilities and thus, trust e-voting less. Moreover, it is not likely that there would be much difference in the familiarity and knowledge of information technology between Master and PhD students of business and economics programs.

The third sub-group we explored was nationality and the only significant result suggests that Germans score lower on the trust in general technology construct and its subconstructs than the Portuguese subjects regardless of the application's version. Even though it seems that Germans trust technology less than Portuguese in general, it has not been reflected in the two remaining constructs, and there was no difference in trust between the two nations across the two versions.

3.2 Focus group findings

In paragraph 5.1, we explained that the lack of trust in blockchain-based voting systems might be caused by a lack of familiarity with the underlying technology. Additionally, the dynamic of the discussion between subjects in our focus group actually revealed that the underlying reason for doubting online voting applications, including but not necessarily implying blockchain-enabled systems, can specifically be attributed to a lack of perceived security. Whereas subjects trusted the system for the sake of a student's election, most of them indicated that they would fear cyberattacks in larger rollouts, i.e. governmental elections. Subject 2 underlined that "Personally, [...] I would not feel safe" when referring to the idea of a use in a nationwide election. Subject 2 elaborated on the aforementioned argument by stating that the main difference between current paper-based systems and digital solutions lies in the centralization which goes along with a „single point of attack". Whereas only a few people are possibly able to „manipulate some votes in different places" in paper-based elections, digitizing the process combines the processing and counting of votes in one single entity and thus, increases the magnitude of a possible attack. These findings manifest the need for a transparent and secure system as well as a high level of people's familiarity with the underlying technology.

This conclusion is evidently backed up by Dogo et al. (2018), who have stressed security as a key requirement for online voting platforms.

Ayed (2017) actually lists some nationwide initiatives which failed precisely due to intolerable security issues and propose a blockchain-based system to resolve these problems. The author highlights that online voting, e.g. blockchain-based online voting systems, has to have even higher security standards as traditional voting mechanism in order to protect the integrity of voters' contributions and achieve widespread adoption.

However, the main challenge seems to be how to effectively communicate a system's features to facilitate adoption. Subject 1 initiated the idea of educating eligible voters on the blockchain technology and its benefits: " [...] they would have to share the advantages of blockchain systems so that everybody is able to understand the technology and its benefits". Subject 2 added an argument, most of the students seemed to agree on: "People will not search for knowledge about it. I think you need to educate people." A popular and solid understanding of the main functionality of an introduced voting system seems to be a necessity to achieve a high level of trust. As has been mentioned in our literature review, Germany actually fixed this requirement legally. The current law determines that every citizen or at least every eligible voter needs to be able to roughly understand the functionality of the election procedure (Seedorf, 2016).

As we have stated in Figure 3 and highlighted in the introduction of this discussion chapter, we experienced a remarkably higher turnout in this year's election at Nova SBE. This observation provides further evidence the first part of our research framework: Online voting encourages participation in elections, which is supported by literature (Breux et al., 2017; Goodman and Stokes, 2018).

Our focus group discussion revealed that transparency can be seen as the key enabler of trust in voting systems, since all of the seven interviewed students agreed on this thought. Six out of seven interviewees actually assented that blockchain can potentially help to enhance transparency, according to the student's own, personal definition of the term.

To provide evidence from literature, Spycher et al. (2011) stress that, despite strong technical achievements for the security of online voting systems, it is more important that these features are exploited and communicated transparently in order to create trust. Dogo et al. (2018) retrieve transparency as a key property of blockchain technology due to its distributed and disclosed nature. These two pillars are the second part of our research framework and help to justify our initial hypothesis: Blockchain technology is able to introduce transparency to online voting systems, hereby enhances their trustworthiness and ultimately helps to increase voter turnout.

3.3 Limitations

Concerning the limitations of our study, three significant aspects have to be mentioned. First, the profile of our sample. Whereas the sample size (n = 454) surpassed our expectations and meets the requirements to manifest a profound outcome, the vast majority of our participants were white (93%), aged between 18 and 24 (83%) and either Portuguese, German or Italian (88%). More importantly, they were all students, either enrolled in a Bachelors, Masters or PhD program related to economics, finance or management studies. One could assume that the affinity and openness of people towards technology and digital transformation processes have a major impact on how they perceive and whether they appreciate our voting system and the application of blockchain technology. Kim et al. (2009) found evidence that consumers' attitude towards mobile applications, as an example of software, is highly influenced by their general affinity towards mobile technology. Since students are generally more likely to show a pronounced level of technical learning than other parts of the population (Surry, 2010), this might have resulted in a bias in favor of our initiative and the measured trustworthiness of our online voting system. However, reflecting on the findings from section 5.1.2, this effect is discussed quite controversially in the literature.

In order to isolate any potential age and education effects on the results, it is highly desirable to run a similar experiment with a randomly selected and thus more representative sample profile.

Second, the lack of information about blockchain technology. Since we deployed Votechain in the student representative election, we handed the ownership of the system over to the school before the elections. The university did not allow us to publish information about the applications technology up until students cast their vote. In addition, notifying voters about the use of blockchain could have jeopardized the unbiasedness of the A/B test. In combination, this means that our prospects were not aware that the system is blockchain-based prior to the elections. Nevertheless, it has to be stated clearly, that students did neither have any incentive nor the chance to inform themselves about blockchain applications before the election. Being informed about the election context could have led to higher familiarity with the technology and thus, higher trust in the system.

In the case of a nationwide implementation of an online voting platform comparable to Votechain, the election authorities would most likely try to educate the population about the utilized technological framework in an easy understandable way. That is why we still believe that blockchain technology bears a high potential to positively impact the trustworthiness of online voting system. It remains up to future research, therefore, to scientifically prove this hypothesis and to investigate whether education and a resulting popular, rough level of technical understanding in the population can further drive trust.

Third, the timing and nature of the study. The Student Representatives Election, which we used to conduct our experiment was limited to a time period of eight hours (9 a.m. - 5 p.m.), during which votes could be casted and the survey could be answered. This means that some students might have had limited time to participate in the election.

However, since 47% of all voters participated in the experiment by filling out the survey, we assume that some did not take sufficient time to evaluate their experience before answering the survey questions. Hence, our results might have been influenced by an indefinite factor of randomness in the answers of some prospects. This argument is actually strengthened by the fact that the application as well as any information and the study itself was conducted in English. Whereas all degrees are taught in English and students are required to meet a reasonable level of fluency, we are still not able to ensure that all participating subjects understood every detail of the study. Hence, there might be some distortion due to a language barrier. Moreover, there was a sampling bias within the experiment, since only 454 out of 967 voters filled out the survey. It is possible that the voters who decided to participate in the survey were already prompted to do so by having prior positive experiences with similar technologies or our application in specific. This would also explain the rather high scores for all subconstructs. Thus, we are unable to draw conclusion about the experience of all participating voters with the help of our results. Lastly, we expressed an incentive for conducting the survey after casting one's vote. Every survey participant was eligible to win a free dinner voucher. Filling out the survey out of a motivation focused on this price may have led to very quick and unthoughtful responses.

3.4 Future research

Our experiment did not provide the intended evidence for the usage of blockchain protocols in online voting systems. However, the focus group discussion provided a reasonable justification, since a lack of familiarity seems to be the key reason for our result. As we have stated at the end of paragraph 5.2, the output of our experiment and focus group lets us remain with our initial research framework. It is up to future research, though, to find evidence that blockchain can actually improve the trustworthiness of online voting applications and procedures in general.

When carrying out required experiments, the samples should be representative collections of subjects, incorporating different point of views of various economic and sociological classes of people in the respective population.

Besides, future research should investigate ways to educate large majorities of the target group of people. Our focus group discussion showed that there is a relatively low level of personal initiative to inform oneself about a technology, although it might be used in relevant elections at some point in the future. Researcher and responsible authorities should therefore develop a suitable strategy to ensure a widespread, rough knowledge about blockchain functionality and benefits in the decentralization of voting systems before such a system is used in public elections.

Internet voting systems moreover provide substantial cost saving potential. Referring back to Estonia as the only nationwide example of an implemented online voting solution, Krimmer et al. (2018) conducted research on the cost comparison of Estonia's multichannel elections and found that internet voting was only half the price of the second cheapest option, the traditional paper ballots. By realizing these cost saving opportunities, governments and authorities are able to free up resources which can be invested in educational programs in advance.

3.5 Lessons for practitioners

Our focus group discussion showed that the option to verify votes after they are cast is very positively influencing the perceived security of the system and thus, its trustworthiness. This proposition would manifest the importance of this function and imply its utilization for practitioners. However, Estonia has provided a cast-as-intended feature in which voters can check if their vote was counted correctly, either. Just 4% of all participating voters actually used the feature, which relativizes it's relevancy (Russell and Zamifir, 2018).

Regarding technical specifications, researchers should identify the most ideal blockchain consensus protocol for its application in voting. Besides, it remains to be answered whether governments should provide all required nodes or if every voter should represent a node and how their mining effort should be compensated. Or should the government even decide to leverage an existing, large scale blockchain like Ethereum as has been done in various initiatives such as SecureVote (Cucurull et al., 2019).

In any case, a voting blockchain at a scale of a nationwide election would obviously consist of a significantly higher number of nodes than a smaller, private election requires. As has been explained in our literature review, a larger network leads to increasingly tamper-resistant chains and thus, increases security.

Concerning display design, online voting initiatives tend to not base their development on scientific design frameworks, e.g. Ayed (2017). However, we recommend to further investigate how the blockchain architecture should best be visualized for the voter and how initiatives to draw attention should most effectively be settled up.

To conclude, our focus group discussion proposed that governments should advisably start with introducing a digital voting mechanism in a smaller extent first before rolling it out on a nationwide level. A good way to do so could be offering eligible citizens living abroad the opportunity to cast their vote online using a scalable online system. According to our focus group, this approach could help to make the broad population of a country familiar with online voting in general and the utilization of blockchain technology hereby. System reliability and security could be proven which would possibly lead to higher degrees of trust and appreciation of associated benefits. This approach has already been picked up by existing blockchain-enabled voting applications like Voatz. The US start-up introduced their system to the public by supporting universities like the University of South Florida, hosting their student body elections in early 2018 (Shine, 2018).

In the same year, they also cooperated with the state of West Virginia to enable military personnel who were involved in an operation outside of the country, to participate in the 2018 Primary Elections (Voatz, 2019a). Since then, Voatz was able to extend their partnerships with several states including Oregon, Utah and the city of Denver, enabling not just military personnel but also people with disabilities to vote remotely (Voatz, 2019b). This indicates a growing interest in online voting systems in general and blockchain-enabled voting applications in specific.

4. Conclusion

Blockchain bears high potential to enhance the transparency of online voting systems and therefore increase their trustworthiness to drive adoption and higher election turnouts. We expected that our A/B-experiment would reveal higher levels of trust for blockchain-enabled voting in contrast to a two-factor-authentication security protocol, which we used for the control group of our experiment. Our results showed the opposite. Although only one of the seven sub-constructs we applied to measure trust showed a significant difference between version A and B, this difference was in favor of two-factor-authentication. Students tended to perceive version A (two-factor-authentication) as more reliable than version B (blockchain-based). However, we were able to retrieve from literature that transparency of online voting systems and familiarity with the utilized technology are key enabler of trust, which is supported by our focus group findings. Students agreed that blockchain enhances transparency which verifies the technology's potential for being applied in online voting.

Therefore, we concluded that people have to become more familiar with blockchain technology to be able to trust its application. The right way to achieve a widespread technical understanding seems to be educating the population ahead of time.

Future research should use our findings to set up an experiment, using a representative sample and effective education methods, to fundamentally approve blockchain's potential in driving the trustworthiness of online voting systems. In times of decreasing turnouts of parliamentary elections and a dangerous shift to the right in global politics, the importance of finding effective ways to engage people in raising their political voice cannot be overstated.

5. Bibliography

Akcora, C.G., Gel, Y.R. & Kantarcioglu, M., 2017. "Blockchain: A Graph Primer." *arXiv [cs.CY]*. Available at: http://arxiv.org/abs/1708.08749.

Amazon Web Services. 2019. "Blockchain in AWS" Accessed September 27. https://aws.amazon.com/de/blockchain/

Apte, S. and Petrovsky, N., 2016. "Will blockchain technology revolutionize excipient supply chain management?." Journal of Excipients and Food Chemicals, 7(3), p.910.

Barcelo, J., 2014. "User privacy in the public bitcoin blockchain." Available at: https://pdfs.semanticscholar.org/549e/7f042fe0aa979d95348f0e04939b2b451f18.pdf.

Bauerle, N. 2019a. "How does Blockchain Technology work?". Accessed September 27. https://www.coindesk.com/information/how-does-blockchain-technology-work

Bauerle, N. 2019b. "What are Blockchain's issues and limitations?". Accessed September 27. https://www.coindesk.com/information/blockchains-issues-limitations

Benchoufi, M., Porcher, R. and Ravaud, P., 2017. "Blockchain protocols in clinical trials: Transparency and traceability of consent." F1000Research, 6.

Biryukov, A., Khovratovich, D. & Pustogarov, I., 2014. "Deanonymisation of Clients in Bitcoin P2P Network." *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*. Available at: http://dx.doi.org/10.1145/2660267.2660379.

Boucher, P., Nascimento, S. & Kritikos, M., 2017. "How blockchain technology could change our lives." *STOA*.

Bruce, J.D., 2014. The mini-blockchain scheme. White paper.

Buterin, V., 2015. "On public and private blockchains." *Ethereum blog*, 7.

Crosby, M. et al., 2016. "Blockchain Technology - Beyond Bitcoin." *Applied Innovation Review*.

Digiconomist. 2019. "Bitcoin energy consumption index" Accessed December 28. https://digiconomist.net/bitcoin-energy-consumption.

Di Pierro, M., 2017. "What is the blockchain?." Computing in Science & Engineering, 19(5), pp.92-95.

Dogo, E. M., Nwulu, N. I., Olaniyi, O. M., Aigbavboa, C. O., & Nkonyana, T. 2018. "Blockchain 3.0: Towards a Secure Ballotcoin Democracy through a Digitized Public Ledger in Developing Countries." i-Manager's Journal on Digital Signal Processing, 6(2), 24.

Eyal, I., Gencer, A.E., Sirer, E.G. and Van Renesse, R., 2016. "Bitcoin-ng: A scalable blockchain protocol." In 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16) (pp. 45-59).

Giese, P., Kops, M., Wagenknecht, S., De Boer, D. and Preuss, M. 2016. Die Bitcoin Bibel: Das Buch zur digitalen Währung. BTC-Echo.

Iansiti, M. and Lakhani, K.R., 2017. "The truth about blockchain." Harvard Business Review, 95(1), pp.118-127.

Hertig, A. 2019a. "How will Ethereum scale?". Accessed September 27. https://www.coindesk.com/information/will-ethereum-scale

Hertig, A. 2019b. "How do Ethereum Smart Contracts work?" Accessed September 27. https://www.coindesk.com/information/ethereum-smart-contracts-work

Hjálmarsson, F.Þ., Hreiðarsson, G.K., Hamdaqa, M. and Hjálmtýsson, G., 2018, July. "Blockchain-based e-voting system." In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 983-986). IEEE.

Jaag, C. & Bach, C., 2017. "Blockchain Technology and Cryptocurrencies: Opportunities for Postal Financial Services." *The Changing Postal and Delivery Sector*, pp.205–221. Available at: http://dx.doi.org/10.1007/978-3-319-46046-8_13.

Kim, Y.A. & Srivastava, J., 2007. "Impact of Social Influence in e-Commerce Decision Making." In *Proceedings of the Ninth International Conference on Electronic Commerce*. ICEC '07. New York, NY, USA: ACM, pp. 293–302.

Kshetri, N. & Voas, J., 2018. "Blockchain-Enabled E-Voting." *IEEE Software*, 35(4), pp.95–99. Available at: http://dx.doi.org/10.1109/ms.2018.2801546.

Lánský, J., 2017. "Bitcoin System." *Acta Informatica Pragensia*, 6(1), pp.20–31. Available at: http://dx.doi.org/10.18267/j.aip.97.

Liang, X. et al., 2017. "Towards data assurance and resilience in IoT using blockchain." In *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*. ieeexplore.ieee.org, pp. 261–266.

Microsoft Azure. 2019. "Blockchain". Accessed September 27. https://azure.microsoft.com/en-us/solutions/blockchain/

Miraz, M.H. & Ali, M., 2018. "Applications of Blockchain Technology beyond Cryptocurrency." *Annals of Emerging Technologies in Computing*, 2(1), pp.1–6. Available at: http://dx.doi.org/10.33166/aetic.2018.01.001.

Moser, M., 2013. Anonymity of bitcoin transactions.

Nofer, M. et al., 2017. "Blockchain." *Business & Information Systems Engineering*, 59(3), pp.183–187. Available at: http://dx.doi.org/10.1007/s12599-017-0467-3.

Osgood, R., 2016. "The future of democracy: Blockchain voting." COMP116: Information Security, pp.1-21.

Pajot-Phipps, S., 2017. "Energizing the Blockchain—A Canadian Perspective." *Bitcoin Magazine*, 26.

Riedlberger, K., 2020. “An Exploration of Blockchain-enabled online voting”. NOVA Schoolf of Business and Economics, Lisbon.

Rizzo, P. 2015. “Filament Nets $5 Million for Blockchain-Based Internet of Things Hardware” Accessed September 27. https://www.coindesk.com/filament-nets-5-million-for-blockchain-based-internet-of-things-hardware

Sasson, E.B. et al., 2014. “Zerocash: Decentralized Anonymous Payments from Bitcoin.” In *2014 IEEE Symposium on Security and Privacy*. ieeexplore.ieee.org, pp. 459–474.

Schaub, A. et al., 2016. “A Trustless Privacy-Preserving Reputation System.” In *ICT Systems Security and Privacy Protection*. Springer International Publishing, pp. 398–411.

Stoll, C., Klaaßen, L. and Gallersdörfer, U., 2019. “The Carbon Footprint of Bitcoin.” Joule.

Szabo, N., 1997. “Formalizing and securing relationships on public networks.” First Monday, 2(9).

Trustnodes. 2017. “Ethereum is now the most secure public blockchain, overtaking Bitcoin” Accessed September 30. http://www.trustnodes.com/2017/05/21/ethereum-now-secure-public-blockchain-overtaking-bitcoin

Twesige, R.L., 2015. “A simple explanation of Bitcoin and Blockchain technology.”

Veuger, J., 2018. “Trust in a viable real estate economy with disruption and blockchain.” Facilities, 36(1/2), pp.103-120.

Viriyasitavat, W. & Hoonsopon, D., 2019. “Blockchain characteristics and consensus in modern business processes.” *Journal of Industrial Information Integration*, 13, pp.32–39. Available at: http://dx.doi.org/10.1016/j.jii.2018.07.004.

Vysna, N., 2020. “Elections and Trust”. NOVA School of Business and Economics, Lisbon.

Wang, H. et al., 2018. “Blockchain challenges and opportunities: a survey.” *International Journal of Web and Grid Services*, 14(4), p.352. Available at: http://dx.doi.org/10.1504/ijwgs.2018.10016848.

Yang, Z., Zheng, K. & Yang, K., 2017. “A blockchain-based reputation system for data credibility assessment in vehicular networks.” *2017 IEEE 28th annual*. Available at: https://ieeexplore.ieee.org/abstract/document/8292724/.